ABSTRACT OF THE DISCLOSURE

[00125] A computing platform (10) protects system firmware (30) using a manufacturer certificate (36). The manufacturer certificate binds the system firmware (30) to the particular computing platform (10). The manufacturer certificate may also store configuration parameters and device identification numbers. A secure run-time platform data checker (200) and a secure run-time checker (202) check the system firmware during operation of the computing platform (10) to ensure that the system firmware (30) or information in the manufacturer certificate (36) has not been altered. Application software files (32) and data files (34) are bound to the particular computing device (10) by a platform certificate (38). A key generator may be used to generate a random key and an encrypted key may be generated by encrypting the random key using a secret identification number associated with the particular computing platform (10). Only the encrypted key is stored in the platform certificate (36).